Objectives

- What DNS is and why we need it
- DNS on Windows® Server® networks / Community Connect
- Troubleshooting

What is DNS?

- A system for translating easily remembered hostnames into their IP addresses (names to numbers)
What is DNS?

• A system for translating easily remembered hostnames into their IP addresses
• A distributed database
• Fault Tolerant
• A “Namespace”
DNS Namespace

Why do we need DNS?

• To locate Active Directory Resources (e.g. to find a Domain Controller for logon)

• To locate pages on the Internet and for email
Why do we need DNS?

- To locate Active Directory Resources (e.g. to find a Domain Controller for logon)
- To locate pages on the Internet and for email
- Connecting to printer shares etc

How Name Resolution Works

Cached lookups
So...name resolution relies on finding a server with “authoritative” data for a domain...

How is this data stored?

Zone Files

- DNS data is divided into manageable sets of data called zones.
- Contain name and IP address information
- Primary and Secondary - `%systemroot%\system32\dns (*.dns)
- Active Directory Integrated
- Forward and Reverse

DNS Zone Transfers
DNS Primary and Secondary Zones

- They’re still out there, they work, however, there are drawbacks:
  - Zone Transfer process problematic
  - Bandwidth/Network Resources
  - Single Point of failure (Primary Server)
  - Improved by Update Notification and Incremental Zone transfers

Active Directory Integrated (ADI) Zones

- Benefits:
  - Less network traffic
  - Multimaster model
  - Clients able to register in DNS more efficiently
  - Less Administrative effort
  - Secure Dynamic Updates
  - No Single Point of Failure

Stub Zones

- A zone with pointers to another domain
- Useful for users needing to access resources in separate Domains
**Stub Zones**

- Usually a DNS Server contacts a Root server on the Internet if it can’t resolve a host name.
- A Stub Zone is a DNS Zone that holds only:
  - A copy of the SOA record for the zone.
  - Copies of NS records for all name servers authoritative for the zone.
  - Copies of A records for all name servers authoritative for the zone.
- Stub Zones streamline name resolution.

**Name Resolution using Stub Zones**

- Client sends recursive query to DNS server hosting stub zone.
- DNS server uses stub zone’s resource records to help resolve query.
- Stub zone identifies authoritative DNS servers for original zone.
- DNS server queries authoritative servers without having to find them first.
- [http://support.microsoft.com/kb/811118](http://support.microsoft.com/kb/811118)

**Forwarders**


Conditional Forwarding

- New feature in Windows Server 2003
- Allows forwarding to DNS servers based on queried domain name
- Examples - forward queries for:
  - reskit.local to 10.0.0.1
  - ad.reskit.local to 169.254.33.9 and 169.254.8.22 and 169.254.8.77
- Like Stub Zones can improve the performance of DNS queries
Stub Zones and Conditional Forwarding Compared

- Stub zones are dynamic, conditional forwarders are static
- Stub Zones can be stored as Active Directory Integrated
- Requires permission from the administrator of the other domain – uses zone transfer
- A stub zone can also be used to keep the DNS server hosting a parent zone aware of all the DNS servers which authoritative for a child zone
- Conditional Forwarders can be used to forward to a specific Name Server (Firewall)

Resource Records

- The “A” Record
  – Used to Map a hostname to an IP address
- The “NS” Record
  – Show which DNS name servers are responsible for the domain
- The “MX” record
  – Indicates which server or servers are responsible for handling mail for the domain
  
  example.co.uk    IN    MX   10     mail.example.co.uk
  example.co.uk    IN    MX   100    mail.connect.co.uk

Resource Records

- CNAME records – make an alias
Resource Records

• The “PTR” Record
  – Maps an IP address to a hostname
  – A “reverse lookup”

Start of Authority Record

• The first resource record in any Domain Name System (DNS) Zone file should be a Start of Authority (SOA) resource record.

Service Lookups
Service Lookups

- **_kerberos**
  - The "data" section of this shows a server that is available to take part in Kerberos authentication (this is the way that Windows servers can securely determine who you are, and what you are allowed to do on the network).
- **_ldap**
  - This shows servers that can be used to query the Active Directory using LDAP (the Lightweight Directory Access Protocol).
- **_pc_**
  - Any servers which can be found with this entry are "Global Catalogue" servers. On a Community Connect network this should be all of your domain controllers.
- **_kpasswd_**
  - This is used to show servers which can be used for Kerberos password changes in the domain.

DNS and Logon

- **Netlogon** service on the client queries DNS for the SRV (Service Location) records
- **LDAP**
- **Kerberos**
- **Global Catalog** - needed for logon in Multi-domain Forest
The twilight _msdcs Zone

- Records beginning with an underscore are for servers to locate resources, for example _GC, means Global Catalog and _DC means Domain controller.
- In Microsoft® Windows® Server 2003 these _MSDICS records have been moved to their own zone.
- Replication can be controlled

Troubleshooting

- NSLOOKUP
- NETDIAG
- DCDIAG
- DNSLINT
- DNSSCMD
- NLTEST
- IPCONFIG
- DNS LOGGING
- (good old…) EVENT VIEWER

NSLOOKUP

- A command-line administrative tool for testing and troubleshooting DNS servers

Specific issues include: Desktop Agent: failed to retrieve any server names from the station location component. Program sets cannot be updated
NSLOOKUP In-Depth

NETDIAG

- Can be used to Verify entries in C:\WINNT\System32\config\netlogon.dns
- These errors indicate missing SRV records:
  - "A domain controller for the domain could not be contacted"
  - "DNS name does not exist", "error code 0x0000232B RCODE_NAME_ERROR"
  - "The DNS SRV records required to locate a domain controller for the domain are not registered in DNS"
- NETDIAG /TEST:DNS and NETDIAG /FIX both very useful!

DCDIAG

- DCDIAG /TEST:DNS can be used to validate DNS health
- Can also be used for some very targeted tests:
DNSLINT
• Download from http://support.microsoft.com/kb/321045
• Provides an overview of DNS health
• dnslint /ad /s localhost /v

DNSCMD
• Create zones and delete zones
• View and update resource records in a zone
• Age of records
• ...and more

NLTEST
• Another command line tool for your troubleshooting armoury
  • You can use with the /dsregdns switch to force a local or remote DC to re-register its' DNS records

IPCONFIG
• Basic diagnostic tool
• Ensure clients are pointing to the correct DNS Server(s)
• Ensure the Forest Root points to itself only
  – IPCONFIG /ALL
  – IPCONFIG /DISPLAYDNS
  – IPCONFIG /FLUSHDNS
DNS Logging

- Scenarios for creating a DNS Debug Log
- Web page not found - 404 error.
- Email delivery error.
- Cannot find a server by its a UNC path.
- Secondary DNS servers do not receive notifications or updates.

DNS Logging

- 20100407 11:56:25 948 PACKET 02A26140 UDP Snd 172.16.10.14 f6f5 R Q [8385 A DR NXDOMAIN] A (8)intranet(3)CC4(3)net(0)
  - NXDOMAIN indicates no record exists
- 20100407 11:56:25 94C PACKET 02A36730 UDP Rcv 172.16.10.14 2bd1 Q [0001 D NOERROR] A (8)intranet(5)Local(0)
  - NOERROR - good news! The query successfully resolved “Intranet”
DNS Server – Event Viewer

• Some common events are:
  – Event ID 2: Indicates that the DNS server has started
  – Event ID 3: Indicates that the DNS server has shut down
• Critical events to look out for:
  – 4000, 4004, 4007, 4014, 4015: Normally indicates that Active Directory and DNS aren’t playing well together. Check the AD is working normally, then restart DNS

Scavenging – why its needed and how to configure it

• Large numbers of stale Resource Records can eventually take up server disk space and cause unnecessarily long zone transfers.
• Name resolution problems on the network (including MSMQ).
• RDP – unexpected result?
• Degradation of server performance
• TEC396803

DNSUpdateProxy

• DHCP Server can be configured to dynamically register client records
• It becomes the owner of the record
• If the server fails other servers may not be able to update the records
• Scavenging period – tells DNS how often to check the zone for stale records
• No-refresh interval – suppresses client re-registration (reduces replication)
• Refresh Interval - the number of days after the No-refresh Interval expires that DDNS will wait for the client to refresh its record before the record becomes stale

• "I'm hitting this 'scavenge now' button like a snare drum and nothing is happening. Why?"
• "I woke up this morning, my DNS zones are nearly empty and Active Directory is sitting in a corner rocking back and forth crying. What happened?"

Other useful tools
• Monitoring DNS with the DNS Console
• Monitoring DNS with System Monitor
• Can't logon or join the domain?
  – Ping: Domain Name, _MSDCS GUID (replication)
Advanced tools

• Connectivity or Configuration?
• Wireshark (formerly Ethereal)
  – http://www.wireshark.org/download.html
• In-depth packet sniffing...

Summary

• “Well over 70 percent of all support calls that come to Microsoft support services that start out as Active Directory or Exchange calls end up being DNS calls”